Form PTO 1449		ATTY. DOCKET NUMBER NITT.0027	SERIAL NUMBER To Be Assigned
U.S. Department of Commerce Patent and Trademark Office		APPLICANT KAMINAGA et al	
Information Disclosure Statement by Applicant		FILING DATE Concurrently Herewith	GROUP 2132

U.S. Patent Documents

Examiner Initial		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE

Foreign Patent Documents

Examiner Initial		DOCUMENT NUMBER	FILING DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION	
							YES	NO

Other Documents (Including Author, Title, Date Pertinent Pages, Etc.)

MP		Smart Card Handbook, pp. 263
		Ross Anderson and Markus Kuhn, "Tamper Resistance -- A Cautionary Note", The Second USENIX Workship on Electronic Commerce Proceedings, Oakland, California , Nov. 18-21, 1996, pp. 1-11
		Marc Joye, Arjen K. Lenstra and Jean-Jacques Quisquater, "Chinese Remaindering Based Cryptosystems in the Presence of Faults", top appear in Journal of Cryptology, pp. 1-5
		Peter Montgomery, "Modular Multiplication Without Trial Division", Mathematics of Computation, Volume 44, No. 170, April 1985, pp. 519-521.

EXAMINER	*[signature]*	DATE CONSIDERED	11/02/04

EXAMINER: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

PTO1449

	ATTY. DOCKET NUMBER	SERIAL NUMBER
Form PTO 1449	NITT.0027	09/931,937
U.S. Department of commerce Patent and Trademark Office	**APPLICANT** KAMINAGA et al.	
Information Disclosure Statement by Applicant	FILING DATE August 20, 2001	GROUP 2132

U.S. Patent Documents

Examiner Initial		DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE
MD		6,049,613	04/11/00	Jakobsson			01/13/98
MD		5,631,960	05/20/97	Likens et al			08/31/95

Foreign Patent Documents

Examiner Initial		DOCUMENT NUMBER	FILING DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION YES	TRANSLATION No
MD		WO 99/67919	06/03/99	PCT			X	

Other Documents (Including Author, Title, Date Pertinent Pages, Etc.)

MD		Ramesh Karri, Kaijie Wu, Piyush Mishra, Yongkook Kim, "Concurrent Error Detection of Fault-Based Side-Channel Cryptanalysis of 128-Bit Symmetric Block Ciphers", Proceedings of the 38th Annual Design Automation Conference, June 18-22, 2001, Proceedings of the Design Automation Conference, New York, pp. 579-584
MD		Dan Boneh, Richard A. DeMillo, Richard J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults", Advances in Cryptology - Eurocrypt '97, International Conference on the Theory and Application of Cryptographic Techniques Proceedings, 1997, pp. 37-51
MD		European Search Report dated June 30, 2003.

EXAMINER _(signature)_	DATE CONSIDERED 11/02/04

Examiner: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant

PTO 1449